arm

# 安全宣言

# 简介

在我们逐渐意识到数据洞察所能带来巨大价值的同时，确保系统安全的战火正在熊熊燃烧。作为这场战役的一部分，科技公司肩上的社会责任早已不再局限于提供产品那么简单了。我们在《安全宣言》中描述了这个由数据驱动的世界所面临的威胁正如何愈演愈烈，并详细指明了对抗这种风险的技术应对方向。此外，我们还探讨了身为"信息革命"守卫者这一责任的本质，讨论了所有技术供应商必需共同支持的"社会契约"。

# 内容

# 前言

## 共生：将人类纳入高效的网络安全


**Mary Aiken博士**

都柏林大学网络心理学家

欧洲刑警组织欧洲网络犯罪中心(EC3)

学术顾问 (心理学)


作为一名网络心理学家，我的工作就是在人类与技术相遇的地方，或者就像有些人所说的那样，人类与技术交汇碰撞的地方给出一些深刻的洞见。

我们已经有了防护性的策略针对现实中的犯罪和商业诈骗，但基于网络的犯罪，我们要做的还很多。截至目前，我们一直聚焦于针对关键基础设施的攻击，但是物联网的互联性意味着我们还要应对面向所有基础设施的攻击。现在，黑客攻击无处不在，入侵者在全球范围内从事针对个人和企业的复杂犯罪活动，物联网让他们有了更多机会出手。

人类本身是安全的第一道防线，但并不是所有人都承担了自己的职责。我们并非都是IT专家，设备安全，系统安全也并不都是默认设置。用户有太多关于网络安全的假想，这让他们产生一种得到保护的错觉——虚假安全。许多攻击之所以能成功，就是因为缺乏相应的防范，缺乏基于设计层面的安全防护，缺乏用户认知。年轻一代的用户更精通数字技术，但与此相矛盾的是，他们对于安全问题则相对更盲目乐观。作为学术专家、设计师、开发人员和工程师，我们需要更多地关心消费者，聚焦技术安全的网络心理学。我们需要一个以人为本的方法，它关注的是人类如何真正使用连接起来的"物"，而不是从技术领域去揣测或期望他们如何去做。

威胁源起方——有组织的犯罪集团、民族国家、跨国组织、小团伙——这些都是人。因此，不论是针对消费者还是网络罪犯，关键任务在于明确人类是如何与科技互动的。迄今为止，努力的重点一直都是技术解决方案，不过创新和设计不可能凭空出现。有一点至关重要，那就是洞悉人类行为在网络领域如何凝聚、变化、放大或升级以及背后的原因。

### 调查思维

我们都需要像行为分析器一样思考问题，考虑方法、动机和机会。方法关系到工具和技术，但动机和机会则是人类所特有的。大部分的安全事故都与人为失误有关——而外部攻击者则专注于利用人类的弱点。他们通常从高层开始：鱼叉式钓鱼攻击越来越倾向于锁定高价值人群，比如CEO。如果这样的攻击得逞，通常会导致目标公司遭受巨额损失。

那么，我们要如何确保人类的网络安全？我们需要获得有关网络行为的独到见解。

分析任何系统中的人为因素都是一个复杂的过程，需要对人类的能力有最基本的了解。我们不能只聚焦于认知维度；我们还需要考虑实体、行为、心理、社会、发展、情感和动机等维度。很少有人从社会及心理学角度去考量网络攻击：攻击者都是些什么人，他们为什么要这么做？

为了应对网络攻击，安全解决方案的设计师和供应商需要考虑网络环境和不断发展变化的网络行为的动态本质。值得一提的是，北大西洋公约组织在2016年宣布网络空间为一个"作战域"——认为除了空中、海洋和陆地，现代战争也有可能在计算机网络上发动。

“网络权威的弱化和地位”意味着在网络空间里似乎没有人能负责，因为在现实中，也没人负责。

那么，对于网络空间，我们能做些什么呢？有想过要管辖和管治网络空间吗？就我而言，我认为可以建立一个像联合国宪章那样的“网络空间宪法”，上面可以这么写：

“我们人民，为了创建一个更加完善的网络社会，树立正义，保障网络安宁，提供共同防务，促进公共福利，并使我们自己和后代得享自由的幸福，特别制定本网络宪法。”

就寻找解决方案而言，我们可以吸取环境运动的经验：环境运动的“预防”原则将保护环境的责任加诸到行业身上。这也可以成为网络空间的原则。保障关键基础设施的安全目前仍然是私营领域的责任，但是对于国家电网，航空管制等行业而言，还是需要一个普遍认同的全球安全标准来管理这些关键的产业体系 。

考虑到不断变化的种种威胁以及技术的快速发展，开发一条适应能力更强、更灵活的研发方案就显得至关重要。与此同时，必要的资金支持也能助力更快速交付相关成果。

**迈向共生**

技术应用也有好坏之别。行业面临的关键挑战在于跟上不断变化的网络威胁。网络攻击的数量和发展进化要求人类智能增强（IA）提供更加精确地解决方案，要将人置于整个流程的中心位置，开发并部署相应解决方案，减轻由于技术发展而造成的安全隐患。

这表明，人们对事件的洞察以及就此展开的合作再加上强大的机器学习和深思熟虑的功能能力，就可以建立一个牢固的基础以减少安全攻击、黑客攻击和（或）侵害，协助确保网络空间的安全，从而保护并确保技术行业今后的活力。

这份宣言将帮助技术领域从不同的角度去思考自己在网络空间里的注意事项，它将扩大我们的讨论范围，提高问题的紧迫程度。

# 健康证明：免疫系统和医疗服务如何大规模地实现物联网安全

**Milosch Meriac**
Arm首席安全研究主管

保障系统安全是一场旷日持久的战争，而我们却经常处于被动状态。在面临网络攻击时，通常我们都会先确定攻击源头，然后采取措施解决问题，以降低未来的风险。数十年来，无论对于传统计算还是移动系统我们一直都采取这样的做法。但是，想想未来物联网交互的复杂性，如果想要实现很好的管理并将其规模化，那么这种旧方法即便有实现的可能，也将是非常困难的。

## 担忧危机蔓延

遏制恶意软件影响的能力至关重要，因为摧毁整个系统可能比恶意软件本身更具破坏力。此外，可能还需要耗费大量的时间查找安全漏洞，并发布经过验证的固件更新。随着物联网技术的广泛应用，包括关键的基础设施网络，简直无法想象彻底瘫痪所造成的巨大后果。

这种情况有点类似于人体如何利用自动的、有针对性的、高效的免疫系统反应来对抗感染。人体感染有可能很快失控，最后不仅原先的目标受到影响，也可能迅速传染周围。医疗服务从这开始介入——提供方法治疗病人，这比纯粹依靠人体本身能更快、更有效地应对感染。

所以，我们有一个很好的模式，仿照人体生物学和医疗系统针对设备攻击设计解决方案。它让我们拥有了一个覆盖全网络的响应机制；将已知的安全漏洞签名映射到设备固件上，减少网络架构、系统、软件所面临的潜在安全风险， 并可以为产品团队提供早期指导。

## 接种

那么，物联网的免疫系统和医疗服务是如何运作的呢？首先，让我们分析一下物联网免疫系统可能的样子。最高级情况下，系统一开始在边缘节点进行检测，利用传感器锁定反常行为。这些边缘节点还包括动态固件执行追踪和性能计数器统计，以捕捉代码和数据访问模式。

就像一个生物免疫系统，这项技术可以观察和监控系统网络流量，鉴别并了解典型行为。带时间标记的内部和外部指标利用的是加密总账，可以存储在本地或网络上的防篡改区域。签名和加密的数据包附带着流量矢量观测结果，会从主要应用收集，成为汇总测量数据，再向中央服务器传送回报。基于流量模式的这些读数，程序执行节点的节点交互和特征可以通过更改或撤消访问密钥和强制隧道到流量过滤主机来隔离或检疫。
如果无法以及时方式加密地证明消息传递状态和控制消息，则不兼容的应用程序可以无线重置或重刷新。这种方法相当于传统的安全监控系统：要求提供一个加密的密码用于重置本地的监控设备，迫使可能受到感染的主机与中央控制器持续通信。通过使用这样一条强制的通信信道，迫使安全监察系统和后端服务器通信，不为网络协议栈所知。

强制隔离的节点作为高级别的缓解措施，可以通过执行现有网络连接协议来实现。这意味着不仅可以防止恶意访问邻近设备，还可以管控感染设备的网络流量和带宽，从而缓解入站和出站的拒绝服务攻击。

在最简单的情况下，网络可以通过虚拟网络标识（VLAN

ID)——通常在受控交换机和路由器的支持下——对网络进行分区。将虚拟网络的概念延展到网状网络或许是有意义的。这样的虚拟网络可以利用安全隧道协议，在网状路由器和云架构之间进行端到端扩展。

### 固件"上门服务"

标准化的空中固件升级 (FOTA)文件格式和网络协议对于采用供应商独立的方式进行设备管理是必需的。FOTA要求包括政策执行和降级保护，这两者现皆可由Arm Mbed最新的Firmware Manifest Format支持，以及IETF 标准化正在进行中。安全即服务供应商只能提供节点和供应商的签名固件；它们无法为固件签名。可以视情况要求它们申请一个由本地管理员提供的加密签名，之后才允许进行固件更新。

### 健康检查

现在，让我们看一看物联网的医疗服务可能是什么样的。有效而持续的系统健康检查可以利用基于系统所捕捉的行为而进行的大数据分析。利用针对设备类型、固件版本、系统事件和导致感染点的事件的流量模式进行的统计分析，确认漏洞。接下来，系统就会采用集中的规则和拦截列表在网络边界阻断已知的恶意签名和流量模式。

此外，医疗服务还可以：

- 触发网络免疫反应，根据基于许多设备交互模式的大数据集计算可能性。
- 代表用户采取行动(比如触发固件更新、隔离节点等)——利用本地设备上一个加密的强制性策略将它们的权利限制在最小。
- 让人工操作员为高级用户消除安全警告 (低概率事故)，必要的时候采取进一步的手动操作，以减轻用户负担。
- 实施策略，让过滤的流量才能访问没有应用补丁的设备，并让设备以更高的延迟安全运转。将此视为与深度封包窥视(DPI) 类似的远程中间人防火墙。
- 可以在信任的边界或网状路由器上采用流量过滤器，保护用户隐私。

与医疗服务相辅相成的是可信雾计算设备，它可以部署在本地网络，以实现更出色的恢复能力和可靠性。设备可能非常简单，只是经过安全强化的低成本无线路由器运行几个轻量级可信的软件流程。或者，它们也可能复杂到是高端防篡改的19英寸机架式服务器，用以为许多可信的高端流程提供服务，同时还能实现强隔离、内存加密和内存认证。

为了更多的重量级应用程序可以在云端或者由所有者按需远程配置可信执行环境 (TEE) 。TEE语义可以延伸到网络，提供一个互不信任并且隔离的计算环境，网络所有者在此不必信任迁移到他的本地网络的云供应商的程序代码 。接下来，云供应商就可以依靠迁移到远程网络 TEE 设备隔间的应用程序的完整性和机密性。

云服务可以使用这些受信任的设备降低延迟作业，计算任务，机器学习，机器学习模型的应用推送到本地网络或从或从本地网络镜像数据，从而为网络中断提供更大的弹性，较低的延迟和更好的用户数据的隐私保护。

为了达成这一目标，应用平台必须保证在同一设备以及网络中运行的多个应用程序和虚拟机器的隔离和安全。它必须防止用户或本地攻击者篡改设备，以免漏出数据/知识产权，或防止通过注入不可信的代码错误地改变设备行为。

在本地网络中拥有这些可信的计算节点，还可以使得高能耗的计算任务从电池供电的节点迁移到插墙式供电的设备上。这就可以大幅延长电池寿命和更高的安全性。

### 小结

我所描述的这种依靠无所不在的物联网免疫系统和医疗服务的技术在3-5年内就会成为现实。通过采用和参考人体内对抗感染的方法，我们可以更快速、更高效地应对针对物联网的安全攻击。因为物联网的部署规模，我们必须具备这类全方位的对策，才能维护系统的信任度，而这项目标已非遥不可及。

# 基于设备的安全模式

**Rob Elliott**

Arm视觉架构总监

如果移动设备可以学习如何深入了解人类，从而更好地保护我们免受黑客和盗贼攻击，那会是一个什么样的场景？建立在这种深入了解之上的认证环境，可以完美地保护人类安全。其实，它并不像你想象得那么新奇，机器学习和人工智能就能帮你办到。

机器学习算法已在工业机器人、无人机、汽车应用和更加智能的家用设备等领域被用以实现新的功能。这些运行在网络和计算机设备上的算法，正在你的移动设备上悄悄发力，优化流程和应用程序，让单元运行得更快速、更可靠、更安全。随着机器学习被越来越多地部署到移动设备上，它将深入而独特地了解这些设备的使用方式。这样一来，它们就会熟知自己的用户，而这种熟悉性就成为了真正可靠的身份认证和安全环境的基础。

### 最好的新朋友

设备内部的行为模式会透露许多有关它们交互对象的信息。为了确定身份，这些信息可能来自物理传感器，比如加速度计；也有可能来自与软件更为微妙的交互。这有可能包括用户与触摸屏的交互方式或者他/她启动应用程序的顺序。例如，一台设备正在试图进行 NFC 支付，但是上下颠倒并且亮度较低(例如在口袋里)，那么就有可能引发警报。同样，警报也可能是以下情况所致：

- 优先系统调用
- 高优先级下高频 CPU 活动
- 反常活动，通常不会以如此高速运行

模式识别能力可让更多系统受惠，这类功能已经常用来防范计算机病毒、算法适应行为和回避侦测的伪装技术。包含在安全套件的机器学习功能，可用于侦测异常行为，协助工程师辨识安全问题。 若要辨识已知攻击，可运用日志来训练类

神经网络，再将网络部署于边缘设备。日志是防范已知问题的实用工具，可加以扩充，使其自动反复训练，以应对新兴攻击手法。完成上述准备之后，设备侦测到入侵事件时，将可快速重新训练并部署网络，以应对新的威胁。

所有这些症状可用于向安全链上的更高级别提供有关攻击向量的关键信息。它们可用于确定某个具体的应用程序或设备是否与意外的行为有关。它们还可用于实施进一步的安全防护，以限制支付交易，比如要求额外的生物识别输入，比如声音或指纹识别，以使支付继续进行下去。

### 学会自主学习

为什么这些措施没有植入设备？从许多方面而言，机器学习还处于应用的初级阶段，当我们开始部署解决方案，就表明我们同时也在重新思考我们要如何将计算从云端分布到设备端，以优化学习算法。现在，机器学习的重点在云端。在那里，服务器筛选从设备端采集的海量数据和信息，以便通过训练流程（通常利用神经网络来实施）找到兴趣模式。这种训练不仅需要数据支持，还需要有关数据细节，判断出这些数据是否为我们想要确定的问题样例数据，正反面的例子都需要。

训练一旦完成，机器学习就可用于从不同的输入以及训练网络中推导信息。可以很简单，如要求在0-1的范围内给出五个输入值，确定要推荐哪个输出值。它也有可能很复杂，如提取来自多个镜头和其他传感器的输入信息，然后就如何操控汽车做出决策。随着使用案例的扩展，推导流程需要更强大的计算能力和更短的延迟时间。

将机器学习应用于设备端以实现更好的安全性。现在，这样的学习流程可以在云端完美实现，云端的计算能力几乎是无限的，不过这也是有代价的，例如响应速度会受到很大影响。但是，当我们将机器学习推向设备端，将有助于降低与云计算相关的带宽、成本和延迟。当我们以更加高效的方式分布计算资源时，我们也会相应提升对移动用户的隐私保护，他们可能并不希望自己的数据在云端被分析。（例如早期指纹识别那个例子——一个习得流程，被保存在本地）。在Arm赞助的一个名为"AI的今世与未来"项目中调查人们对待AI的态度，调查发现，人们渴望对一些敏感数据进行本地控制。

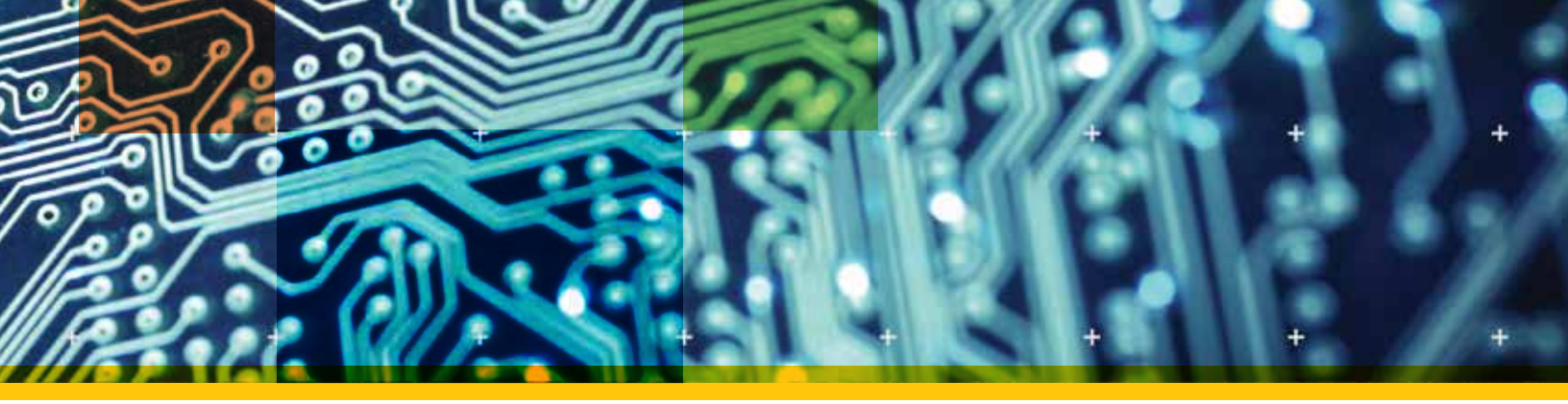
随着传感器数量的激增，现在已经能够捕捉海量数据的设备将在未来捕捉到更多数据。这需要在设备端具有更加强大的计算能力，因为越来越多的数据将会保存在这里。这些数据将被纳入一组最新的权系数组。随后，这些最新的权系数也可以跟一个基于云的系统共享，从而在设备之间分享信息，针对这些数据执行不同的计算任务。这种协作方法创建了一种强大而高效的学习方式，让诸多设备分摊这种工作。人们对更高性能和更低延迟的需求催生了对出色的硬件、软件和工具的渴望。这些都是 Arm 一直在努力的方向。接下来带大家看一看在软件领域 Arm的成绩。

> **熟悉度是真正坚实验证的基础……**

### 使软件有意义

机器学习的软件环境经常令人感到困惑。因为有大量的机器学习框架，在不同的性能层级都有多个学习库的支持；有大量的设备，有许多部署方法，从运行完整的框架到运行一个定制的转换工具。为了简化这些步骤，Arm提供了一个软件和工具平台，让这个体验变得更简单、更一致。另外，我们确保像Tensorflow和Caffe这样已经被采用的工具将会以一种创造性的方式完美运转。

想要简化这个过程，那么有一个能提供简便机器学习部署路径且稳定可靠的软件平台就是关键所在。随着更多的新设备出现，这个软件平台要能够保证在编写软件时无需做出重大修改，而且在这个平台上对学习库进行优化后，还可以实现它所需要的更多硬件创新，同时实现在Arm平台上进行无缝的软件部署。



# 提升代码安全的架构方向


## Richard Grisenthwaite

Arm首席架构师兼研究员


在黑客与其攻击目标争夺致胜先机的激烈角逐中，CPU架构通过引入全新的预防设施来回应已知的攻击。攻击者则回应以更加复杂的攻击，不断循环往复。但是，我们现在正站在一个全新阶段的起点，这个循环有可能在此期间被打破，或者至少将循环周期大大拉长。这个全新时代需要硬件和软件开发人员的共同努力，为了提升安全性以前所未有的姿态开展合作。

### 应对“假数据”

现在，攻击会利用处理器使用的数据来破坏正常执行状态。通常情况下，正在被处理器使用的数据会被写入堆栈上的缓冲区。攻击者将写到堆栈的数据同时变成可执行的代码序列。通过颠覆返回功能，比如，通过缓冲区溢位就可以破坏函数返回，处理器就可能被骗去执行任意及潜在恶意的代码。

为了应对这个问题，大约从2000年开始，处理器架构开始引入新的功能，将内存区域(包括堆栈)标记为“不可执行”。Arm的Armv6架构开始支持从不执行位(XN)。一时之间，大家认为这个问题已经得到了解决。但是，攻击者想出了新的花招，比如“返回至 C 标准库攻击 (return-to-libc)”和“返回导向编程 (return-oriented programming)”，再一次让利用缓冲区溢出漏洞成为可能。这两种方法都利用缓冲区溢位首先破坏处理器的执行操作，导致它去执行合法安装在内存并被标记为可执行的代码。这使得攻击者可以在意想不到的时候，利用意想不到的数据去运行这些合法的代码。在返回至C标准库攻击中，破坏进程利用“假数据”调用一组带标准库函数，因此允许攻击者使用原始程序不希望的数据来实现其控制下的功能。攻击者通过将标准库代码的片段串在一起来创建“小工具”，从而允许创建几个任意的返回地址列表描述的恶意程序，从而进一步进行面向返回的编程。软件对此的回应是在内存中对库的布局进行随机化处理，增加构建一个这样列表的难度。反过来，攻击者发现了探查地址布局的机制，能够将其实际布局纳入返回地址列表。

### 指针验证防范流氓操作

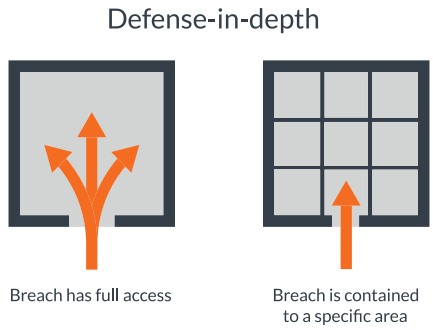
在Armv8.3中，Arm推出了一种全新机制，以进一步提升针对这种攻击的防范级别。这种机制就是指针验证，它利用64位目标地址的部分高位，组成一个加密生成的指针验证码(PAC)。接下来，这个验证码可用于在地址被使用之前对其进行验证。例如，如果处理器在一个返回地址被推到函数入口时添加了PAC，那么它接下来就可以在返回之前检查该PAC是否正确。

其他的属性让这个方法变得更加强大。例如，每一个运行会话都利用独一无二的密钥和一个加密的强函数来生成PAC，让攻击者不可能就给定的返回地址猜出PAC。为了防止递增式地猜测PAC值，操作系统可以通过改变密钥来应对大量的PAC验证错误。

### 深度防御和区隔化

身为 CPU 架构师，我们无法基于这样的原则进行设计——即便是正确编写的软件，也没有机制可以破坏进程的安全性和完整性。我们需要进一步的机制实现 “深度防御”，在周边安全墙内额外树立起来的墙。添加深度防御的有效手段就是改进软件“区隔化”的方式。如果一开始执行操作就被破坏，它确

保还有屏障增加攻击者进一步动作的难度，从而增强了现有的攻击防范机制。为了树立这些屏障或墙，我们需要扩展经典的特权和安全模式，就目前的大多数处理器而言，它们在过去20多年来都没有太大变化。这种经典模式为一个流程提供单一的地址空间，由一组页表进行映射，而且通常被统一授权。对于应用程序的开发人员而言，这种模式非常方便，但对攻击者来说也很方便；如果一个进程被破坏，它可以访问的所有内存空间也就对攻击者开放了。为了避免这种情况，我们将应用程序划分为几个不同的区隔 (有时候也叫"沙箱")。在每个区隔运行的代码只能访问应用程序内存的一个子集，而这个子集是它执行自身功能所必需的。这就意味着区隔内的破坏只限于该区隔能够访问的内存。




现在的处理器对这种区隔化提供不了什么硬件支持，在必要的时候，通常是每个进程在操作系统层面变成一个隔离区。所以，我们借鉴了操作系统进程模型的现有设施来进行区隔化，隔离区之间的通信由标准的跨进程通信机制来实施。每个隔离区内的代码只能访问整个应用程序所使用的转换表的一个子集，从而保护隔离区内代码所使用的内存。尽管在处理器的架构内部缺少特定的支持，至少有一些商业部署的操作系统已经开始采用这个方案，接受了它额外的复杂性——这恰好证明了安全的重要性。未来的处理器架构应该简化隔离区的使用，彻底实现单个进程和地址空间内部的区隔化。

## 管理软件面临的挑战

大部分处理器的标准特权模式提供了特权单调递增的特权级别 (或保护环)。在这种模式中，在一定特权级别运行的代码可以访问较低级别的所有设施，但是该级别至少有一些设施是较低级别无法访问的。这就创建了一个真正的特权层次结构，称为监控软件的基础，比如操作系统和管理程序，它们负责管理在较低级别运行的资源和软件。但是，这也使监督软件成为攻击者非常有吸引力和明显的目标。尤其是，管理软件的主要目的就是管理不同应用或虚拟机器之间的硬件资源。因此在当前的计算模式下，管理软件必需能够读写属于应用程序或虚拟机的数据。这是一个自然而然的方法，但它意味着如果监控软件被破坏，属于正在运行的应用程序或虚拟机器的所有数据也同样被破坏，几乎没有什么余地去保护这些数据。正如我前面所论述的，区隔化有所帮助，但对于未来的系统，我们需要保护应用程序或虚拟机内部的数据，免受来自管理软件的有害入侵，同时无损监控软件有效管理系统的能力。

## 侧信道的兴起

该架构定义了处理器所需的功能性行为，但对于该行为是如何实施的甚少涉及。通常情况下，这对于软件来说无足轻重。该微架构和处理器的物理实现决定了该行为是如何实施的。这种抽象使得架构兼容的软件可以在许多不同的实现上运行。但是，这种抽象太过简单，利用被一般称为"侧信道"的这种机制，就可以让这种微架构和物理实现被攻击者用来破坏安全性。这些攻击依靠的属性不是由架构定义的，这样一来，架构就很难应对这些攻击。不过，它还是有方法帮上忙。例如，显而易见的是——必需要让密钥算法的访问模型和执行时点与该密钥无关。架构可以为此提供帮助，架构可以通过例如提供用于加速公共密码算法的指令来帮助，以避免需要具有依赖于数据的数据访问。在 Armv8.4 中，Arm 引入了一种机制，软件可以用来指示当前代码需要独立于正在处理的数据的时序。

现在，我们开始重新审视专门技术各自为阵的这种局面，它在很长的时间里造成了设备和系统设计的分离。我们之所以这么做，是因为如果想要改变这场无休无止的攻击-修补战的格局，我们别无选择。我们需要硬件和软件团队通力合作，不断提升安全级别。

# Arm宣言

## 履行物联网数字社会契约

**Simon Segars**
Arm首席执行官

根据劳合社 (Lloyd's of London) 的预估，因为各个领域的系统和设备安全通常都不够好，网络犯罪每年致使全球经济损失五千亿美元。

我们在这份宣言中针对技术进步提出了一些想法，它们将有助于阻击网络攻击，但仅凭创新是无法解决这个问题的。正如Mary Aiken在前言中所提到的那样，用户是设备的第一道防线，所以他们就要学着避开可疑网站，下载东西时谨慎小心，记得修改默认密码，并且要让自己的设备安装最新的安全修补程序。

尽管用户应该为了自身的安全承担更多责任，但我们也知道人们通常会做一些有损自身网络安全的事情，可能是无心之举，也有可能是因为他们手头正忙或被分了心。所以，作为技术供应商，我们必须遵循"数字社会契约"(以下简称"社会契约")，承担起自己肩负的责任，无论怎样都要尽力保护用户。

### 安全社会契约

随着互联设备的普及，所有技术公司按照安全社会契约所肩负的责任也与日俱增。网络攻击者越来越狡猾，所以我们必须在设计中将安全视为首要考量因素，根据面临的威胁不断升级安全防御系统。这一社会契约将为技术领域和用户之间的相互信任奠定深厚的基础。

### 违反契约

在 2016 年的 Mirai 僵尸网络攻击中，黑客利用少数日常物联网设备中的安全漏洞攻击网络，发出的数据请求让主要的视频播放和社交媒体网站陷入瘫痪。这些攻击针对的是Dyn，这是一家位于美国的域名服务器 (DNS) 公司，专为外部网络域名提供托管服务。事情发生之后他们当即损失了14,500名客户[1]。

作为一家技术公司的首席执行官，我深知但凡有一家公司或一个个人仰赖我们的技术，Arm就必须维护这份社会契约。我们尽全力解决这个问题，但我们还可以做到更多，比如我们刚刚发布的平台安全架构PSA（Platform Security Architecture），可以指导安全设备实施。此外，我们还在想如何利用生态系统提供设备之间的联通以及在遭到攻击时系统的透明度，确保错误不会再次出现。

### 对安全至上型市场的影响

公司所在领域不同，履行社会契约所面临的挑战也有所不同。看一看汽车市场，这个有着百年历史的领域正在经历一场重大变革，面向大众市场的电力和混合动力汽车以及全自动驾驶汽车正日益成为该行业未来的发展方向。

过去，汽车公司从产品设计到交付要花7-10年的时间。现在，科技公司之间激烈的竞争大大缩短了新产品的创新周期，现在产品的上市速度至少是之前的两倍。但目前的竞争形势有可能对社会契约产生负面影响。不过，汽车行业受到功能安全标准的约束，它们要确保车辆能够满足严苛的安全指标。在这种情况下，社会契约因受到法律保护而得到了加强。所以，当汽车制造商正在学习如何更快速走向市场的时候，技术公司也在学习如何在一个管制更严格的安全环境下行事。

确实，业界面临的一个很大挑战就是互联汽车，安全社会契约在这个领域受到了威胁。最可怕的事情就是汽车的安全系统被黑客入侵，汽车遭到了攻击。虽然没有出现什么违法的

事情，但消费者对商家的信任会因此大打折扣，所以我们一定要更加谨慎小心。

## 加速上市的物联网模式

当加速上市成为重中之重，社会契约所面临的风险也就变得更大。它会影响所有的市场，对商业市场和关键基础设施领域的破坏力可能更强，因为对这两个领域来说，一旦遭到攻击，损失的成本可能会更高。美国能源部今年的遭遇就证明了这种威胁愈演愈烈。当时，他们警告说电力系统面临着重大的网络攻击[3]，而且攻击的"复杂程度、强度和频率"都在不断上升。此外，在过去一年里，美国新成立的国家网络安全中心报告了大约 600 次"严重"攻击[4]，预防了数千次。

所以，随着互联技术的广泛应用，我们必须要重新思考。在强调快速上市的领域，成功建立在设计、出货、分析和转型与加速学习的迭代。但是，这种模式可能有损安全，因为产品的漏洞在大规模应用之后可能就没办法修正，系统就很容易受到攻击。要在讲究快速设计、快速迭代的市场改进这一模式是很困难的，因为很难做到强健的安全防护，它会增加大量时间和金钱成本。所以，尤其是在一个像物联网这样火爆的市场，唯一可能的改变方法就是思考如何实现一种更具恢复能力的商业模式，它不会影响到上市时间，又为开发人员提供安全设计技术。它也会为物联网创建一种全新的商业模式，我们相信这种模式能够与社会契约责任完美契合。

## 设计、出货、分析、改进或隔离和处理：物联网的全新商业模式

在这种新模式下，想要破坏设备安全就不容易了，而且防御系统在遭到攻击时会有更多反应时间。我将这种模式总结为：安全设计、出货、分析、自愈或隔离和处理(如有必要)。对于IoT这类可能需要在单一系统部署大量联网设备的市场，这种模式将成为一大关键。它将提供更精密的模式来保护系统完整性，同时确保科技业对产品生命周期负起责任。

我所描述的这种模式涵盖了修补全体设备的能力，例如修复智能手机中出现的bug，虽然这也不是什么新鲜事。但这种模式可以像医院的外科手术那样对单个设备进行隔离和处理，直到恢复正常，这才是它的创新之处。这种全新商业模式的关键在于分布式智能。它意味着将现在主要出现在云端的那种强大的计算能力运用到设备网络端。这就将我们从指挥-控制这种固定的结构转向一种更加灵活而分散的安全模式。它正好与 Milosch 在免疫系统和医疗服务管理方面的想法不谋而合。从生物学来看，人体免疫系统帮我们抵御着大部分病毒入侵，但医疗服务同样也可以。医疗服务可以实现大规模免疫计划、直接与医生对接，或者是从DNA层面精准解决人体问题。

## 没有标准？

你可能已经注意到我们在对全新的物联网安全模式的展望中没有提及标准。我并没有忽略标准，而是想让各个行业，政府，甚至是联合国来制定这些标准，就像现在联合国已经将网络空间视为战场。

不过在Arm，我们认为标准和政府法规描述的都是相对过去而言，在一个如同物联网一样瞬息万变的世界里，我们需要去定义明天。比起产品的制造者，黑客的速度更快，所以我们的方案必须具有预见性、灵活性和韧性。让我们再次回到免疫系统这个类比：这个系统需要应对它前所未见的威胁，就像白细胞是如何攻击被它们视为威胁的异物。

## 目标

根据分析公司Gartner调查显示，到2017年底，互联设备的使用情况将达到84亿，同时还预测三年后，该数字将超过200亿，实现150%的增长。所以虽然目前网络犯罪就已经造成了高达4,000亿美元的损失，但相比于未来万亿台互联设备带来的潜在风险损失，还真是小巫见大巫。

所以我认为，此份安全宣言中提出的方法和思考将会给人类带来巨大改变，而且我也能预见，在未来我们一定能抵御黑客入侵。

社会契约理论几乎和哲学本身一样古老，指的是人的道德和/或政治义务取决于他们为了组建自己身处其中的社会而达成的契约或协议。
来源：http://www.iep.utm.edu/soc-cont/

1. https://securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/
2. https://www.wired.com/story/car-hack-shut-down-safety-features/
3. https://www.bloomberg.com/news/articles/2017-01-06/grid-in-imminent-danger-from-cyber-threats-energy-report-says
4. http://www.bbc.com/news/uk-41478608
5. https://www.gartner.com/newsroom/id/3598917

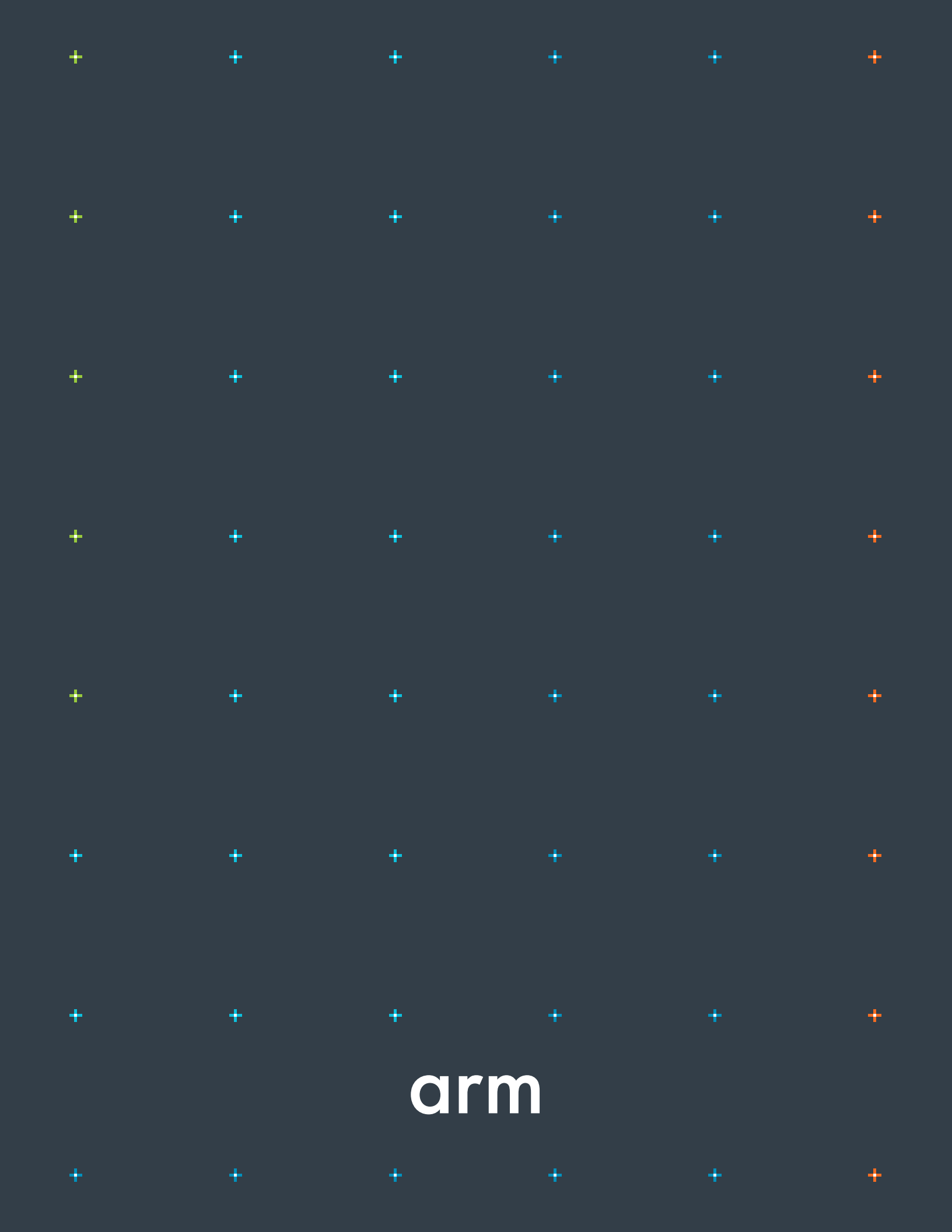
arm

我们正目睹着网络攻击在关键的基础设施领域，医疗健康服务领域轮番上演，大笔赎金将我们压榨到喘不过气。而家用电子设备是黑客作案的一个入口，作为一个行业，我们正站在一个十字路口，一条路是令人惊慌失措且代价不菲的猫鼠游戏，飞速的技术进步不断带来破坏同时又不断地进行修补。另一边，则是一条被诸多共同信仰照亮的全新道路。

# 安全宣言

- 我们在不断拓宽这个互联世界的同时，必须唤起信任
- 任何一家公司都要遵守与用户达成的社会契约
- 安全是行业的集体责任，既是机遇，又是挑战
- 先进的安全智能应该分布到整个物联网产业
- 安全必须是设计的首要考量因素，同时还要提供持久的防护
- 我们必须建立安全体系，解决人类的潜在风险

下载Arm公司的物联网安全宣言：
http://pages.arm.com/iot-security-manifesto.html


arm